**Trust Enumeration Notes**

Reference http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/

The purpose of establishing a trust is to allow users from **one domain to access anothers** resources (like the local Administrators group on a server), to be nested in groups, or to otherwise be used as security principals in another domain (e.g. for AD object ACLs). One exception to this is **intra-forest trusts (domain trusts that exist within the same Active Directory forest)**- any domain created within a forest retains an **implicit two-way, transitive trust relationship with every other domain in the forest**. This has numerous implications which will be covered later in this post

**[IMPORTANT]**“[*A transitive trust extends trust relationships to other domains; a nontransitive trust does not extend trust relationships to other domains.*](http://technet.microsoft.com/en-us/library/cc759554(v=ws.10).aspx)”

This means that transitive trusts can be chained, so users can potentially access resources in multiple domains. Meaning, if domain A trusts B, and B trusts C, then A implicitly trusts C.

trusts can be one-way or two-way. **A bidirectional (two-way) trust is actually just two one-way trusts**

A one-way trust means users and computers in a *trusted domain* can potentially access resources in another *trusting domain*. A one-way trust is in one direction only, hence the name. Users and computers in the *trusting* domain can not access resources in the *trusted* domain.